

COPY OF PAPERS
OFFICIALLY FILED

2181
#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Yoshihito Taninaka and
Noriaki Ohura

Appl. No. 10/092,814

Filed: 03/07/2002

For: SECURITY LEVEL
INFORMATION OFFERING
METHOD AND SYSTEM

:
:
: Group Art Unit: 2181
:
:
:
:
:
:
:
:

RECEIVED

JUN 18 2002

Technology Center 2100

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Certificate of Mailing Under 37 CFR §1.8(a)

I hereby certify that this correspondence is being
deposited on 6/3/02 with the United States Postal
Service as first class mail in an envelope properly
addressed to COMMISSIONER OF PATENTS AND TRADEMARKS,
Washington, D.C. 20231.

6/3/02
Date of Certificate

Cheryl M. Matticks
Cheryl M. Matticks

CLAIM FOR PRIORITY

In the inventors' Declaration filed March 7,
2002, the Applicants in the above-identified application
claimed the benefit of priority under 35 U.S.C. §119 of
their Japanese Application No. 2002-010888. Pursuant to
§119 and 37 C.F.R. §1.55, we are filing herewith a
certified copy of the Japanese Application No. 2002-010888
filed 01/18/2002.

Respectfully submitted,

DANN, DORFMAN, HERRELL AND SKILLMAN
A Professional Corporation
Attorneys for Applicant(s)

By [Signature]
ROGER W. HERRELL, ESQ.
PTO Registration No. 22,964
1601 Market Street - Suite 720
Philadelphia, PA 19103-2307
Telephone: 215.563.4100
Facsimile: 215.563.4044

Enclosure: Priority document



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 1月18日

出 願 番 号

Application Number:

特願2002-010888

[ST.10/C]:

[JP2002-010888]

出 願 人

Applicant(s):

株式会社チームガイア

RECEIVED

JUN 18 2002

Technology Center 2100

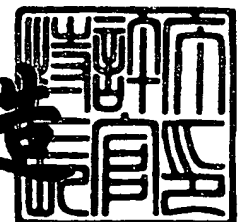
CERTIFIED COPY OF
PRIORITY DOCUMENT

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 3月15日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3017105

【書類名】 特許願

【整理番号】 Y02B002

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 19/00

【発明者】

【住所又は居所】 東京都品川区上大崎3丁目14番37号 株式会社チームガイア内

【氏名】 谷中 義人

【発明者】

【住所又は居所】 東京都品川区上大崎3丁目14番37号 株式会社チームガイア内

【氏名】 大浦 則昭

【特許出願人】

【住所又は居所】 501006882

【氏名又は名称】 株式会社チームガイア

【代理人】

【識別番号】 100104215

【弁理士】

【氏名又は名称】 大森 純一

【選任した代理人】

【識別番号】 100104411

【弁理士】

【氏名又は名称】 矢口 太郎

【手数料の表示】

【予納台帳番号】 069085

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 セキュリティレベル情報提供方法及びシステム

【特許請求の範囲】

【請求項 1】 (a) 特定の機器の環境情報に基づいて、この機器についての脆弱点を特定し、この脆弱点の情報を前記機器に関連付ける工程であって、この脆弱点の情報は、この脆弱点の脅威レベル値を含み、

(b) 特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出する工程と

(c) 前記 (b) 工程で求めたセキュリティレベル値に基づいてセキュリティレベル情報を出力する工程と

を含むことを特徴とするセキュリティレベル情報提供方法。

【請求項 2】 請求項 1 記載のセキュリティレベル情報提供方法において、さらに、

(d) 当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出する工程を有し、

前記 (c) 工程は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項 3】 請求項 2 記載のセキュリティレベル情報提供方法において、さらに、

(e) ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出する工程を有し、

前記 (c) 工程は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項 4】 請求項 1 記載のセキュリティレベル情報提供方法において、

前記(c)工程は、

(b)工程で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである

ことを特徴とするセキュリティレベル情報提供方法。

【請求項5】 請求項1記載のセキュリティレベル情報提供方法において、

前記(c)工程は、

当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現する工程を含むものであることを特徴とするセキュリティレベル情報提供方法。

【請求項6】 コンピュータシステムのセキュリティレベルを算出するシステムであって、

監視対象のコンピュータシステムの環境情報を格納する環境情報格納部と、

更新された各種脆弱点情報であって少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、

前記環境情報に基づいて当該監視対象のコンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と

この脆弱点情報に基づいてシステムの管理者が修正作業を行ったかの情報を格納する脆弱点修正情報格納部と、

特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部と、

前記算出部で求めたセキュリティレベル値に基づいてセキュリティレベル情報を生成し出力するセキュリティレベル情報生成部と

を有することを特徴とするセキュリティレベル情報提供システム。

【請求項7】 請求項6記載のセキュリティレベル情報提供システムにおいて

さらに、

当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出するセキュリティレベル値比較部を有し、

前記セキュリティレベル情報生成部は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を生成するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項8】 請求項7記載のセキュリティレベル情報提供システムにおいて

前記セキュリティレベル値比較部は、ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出するものであり、

前記セキュリティレベル情報生成部は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項9】 請求項6記載のセキュリティレベル情報提供システムにおいて

前記セキュリティレベル情報生成部は、

前記セキュリティレベル算出部で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである

ことを特徴とするセキュリティレベル情報提供システム。

【請求項10】 請求項6記載のセキュリティレベル情報提供システムにおいて、

前記セキュリティレベル情報生成部は、

当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現するものであることを特徴とするセキュリティレベル情報提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えば、ネットワークに接続されたコンピュータシステム群のセキュリティレベルをリアルタイムで正確に評価し提供することができる方法及びシステムに関する。

【0002】

【従来の技術】

最近、クラッカー等により企業や官公庁のネットワークやサーバが攻撃されたり、新種ウイルスに感染するという被害が多発している。このことにより、ネットワークセキュリティの強化に注目が集まっている。ネットワークセキュリティを強化するには、ネットワーク及びこのネットワークに接続された自社機器のセキュリティレベルを絶えず正確に把握しておく必要がある。

【0003】

セキュリティレベルを評価するパラメータとしては、ネットワークやコンピュータのハードウェア及びソフトウェア的な構成といった静的な要素と、日々発生する脆弱点情報に応じて発生しそれに対応することによって変動する動的な要素とがある。企業活動にITを利用する企業にとっては、この動的な要素に迅速に対応しなければ経営リスクが無限大に拡大することになるため、経営者にとってもその管理が非常に重要な課題となっている。

【0004】

【発明が解決しようとする課題】

しかしながら、従来、このセキュリティレベルの把握はシステム管理者に任されており、経営者は、このシステム管理者からの報告を信じるしかなかった。一方、システム管理者の業務怠慢によりセキュリティレベルが低下等する場合もあり、このような要因を含めたセキュリティレベルの管理は非常に困難であった。

【0005】

一方、経営者自身が、膨大なセキュリティ情報から自己のシステムに必要な情報を見つけ出して把握し、しかもその対策をタイムラグ無く施すことは専門技術

的に過ぎるため極めて困難である。

【0006】

この発明は、このような事情に鑑みてなされたものであり、経営者等、セキュリティに関して十分な知識を有さない者であっても理解できるようなセキュリティ情報を、システム管理者の採った作業を反映して、迅速に提供できるシステム及び方法を提供することを目的とする。

【0007】

【課題を解決するための手段】

上記課題を解決するため、この発明の第1の主要な観点によれば、(a) 特定の機器の環境情報に基づいて、この機器についての脆弱点を特定し、この脆弱点の情報を前記機器に関連付ける工程であって、この脆弱点の情報は、この脆弱点の脅威レベル値を含み、(b) 特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出する工程と、(c) 前記(b) 工程で求めたセキュリティレベル値に基づいてセキュリティレベル情報を出力する工程とを含むことを特徴とするセキュリティレベル情報提供方法が提供される。

【0008】

このような構成によれば、未対応の脆弱点情報が存在する場合、機器の種別、その脆弱点の脅威レベル及び未対応の日数に基づいてセキュリティレベル値を算出し、それに基づいてセキュリティレベル情報を生成することができる。

【0009】

また、この方法は、さらに、(d) 当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出する工程を有し、前記(c) 工程は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが好ましい。

【0010】

このような構成によれば、特定の機器に関連付けられた脆弱点情報が複数ある

場合、そのうちもっとも脅威度の高い脆弱点情報に基づくセキュリティ値を当該機器のセキュリティ値とすることができる。

【0011】

この場合、さらに、(e) ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出する工程を有し、前記(c)工程は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが望ましい。

【0012】

このような構成によれば、複数の機器がネットワークに接続されている場合、上述のようにして求めた各機器のセキュリティ値に基づいて、ネットワーク全体のセキュリティ値を算出することができる。

【0013】

さらに、この発明の1の実施形態によれば、前記(c)工程は、(b)工程で求めたセキュリティ値と、機器やネットワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである。

【0014】

更なる別の1の実施形態によれば、前記(c)工程は、当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現する工程を含むものである。

【0015】

このような構成によれば、当該システム若しくはネットワークが満たすべきセキュリティ値の基準値を定めておき、これとの比較で現在のセキュリティ値を表わすことができる。このことで、自社のセキュリティレベルの基準値を明確に把握していない経営者であっても、現在のセキュリティレベルが基準値との関係で相対的に表されるから容易に理解することができる。

【0016】

また、この発明の第2の主要な観点によれば、コンピュータシステムのセキュリティレベルを算出するシステムであって、監視対象のコンピュータシステムの

環境情報を格納する環境情報格納部と、更新された各種脆弱点情報であって少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、前記環境情報に基づいて当該監視対象のコンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と、この脆弱点情報に基づいてシステムの管理者が修正作業を行ったかの情報を格納する脆弱点修正情報格納部と、特定の機器について、この機器の種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応の日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部と、前記算出部で求めたセキュリティレベル値に基づいてセキュリティレベル情報を生成し出力するセキュリティレベル情報生成部とを有することを特徴とするセキュリティレベル情報提供システムが提供される。

【 0 0 1 7 】

このような構成によれば、前記この発明の第 1 の観点に係る方法を実施することが出来るシステムが提供される。

【 0 0 1 8 】

なお、このシステムはさらに、当該機器に関連付けられた未対応の脆弱点が複数ある場合、各脆弱点に関するセキュリティ値を比較し、各脆弱点のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該機器のセキュリティ値として算出するセキュリティレベル値比較部を有し、前記セキュリティレベル情報生成部は、当該機器のセキュリティ値に基づいてセキュリティレベル情報を生成するものであることが好ましい。この場合、前記セキュリティレベル値比較部は、ネットワークに接続された機器が複数ある場合、各機器に関するセキュリティ値を比較し、各機器のセキュリティ値のうち最も脅威度の高いセキュリティ値を当該ネットワークのセキュリティ値として算出するものであり、前記セキュリティレベル情報生成部は、当該ネットワークのセキュリティ値に基づいてセキュリティレベル情報を出力するものであることが望ましい。

【 0 0 1 9 】

また、この発明の他の 1 の実施形態によれば、前記セキュリティレベル情報生成部は、前記セキュリティレベル算出部で求めたセキュリティ値と、機器やネッ

トワークの基本構成等に基づいて算出した基本セキュリティ情報とに基づいてセキュリティ情報を出力するものである。

【 0 0 2 0 】

さらに、この発明の他の 1 の実施形態によれば、前記セキュリティレベル情報生成部は、当該システム若しくはこのシステムが接続されたネットワークのセキュリティ基準値との比較で前記セキュリティ値を表現するものであることが望ましい。

【 0 0 2 1 】

なお、この発明の他の特徴と顕著な効果は次の発明の実施形態の項及び添付した図面を参照することによって、より明確に理解される。

【 0 0 2 2 】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づき説明する。

【 0 0 2 3 】

図 1 中 1 で示すのがこの実施形態に係るセキュリティレベル情報提供システムであり、図 1 はこのシステム 1 の概略構成図である。

【 0 0 2 4 】

このシステム 1 は、ユーザ A 及びこのユーザ A の監視対象コンピュータシステム 6 に関する各種情報 7 ～ 1 1 を格納するユーザシステム DB 2 と、コンピュータシステム 6 の脆弱点に関する情報 2 4 を格納する脆弱点 DB 3 と、前記ユーザシステム DB 2 に格納された各種ユーザ情報 7 ～ 1 1 に基づいて前記脆弱点 DB 3 内の脆弱点情報 2 4 をユーザ A 側に提供すると共にそのセキュリティレベルを算出する脆弱点監視処理部 4 と、前記脆弱点情報 2 4 を生成し前記脆弱点 DB 3 を更新する脆弱点 DB 更新部 5 とからなる。

【 0 0 2 5 】

ユーザシステム DB 2 には、ユーザ毎に、前記コンピュータシステム 6 の環境情報 7 と、システム管理者情報 8 と、組織情報 9 と、脆弱点修正情報 1 0 と、セキュリティレベル値 1 1 とが格納される。

【 0 0 2 6 】

コンピュータシステム環境情報7としては、図2に示すように、コンピュータシステム名、管理者、設置場所、用途等の属性情報12の他、CPU種別やメモリ容量等のハードウェア構成13、OS名やアプリケーションプログラム名等のソフトウェア構成14、起動サービス等の設定15、利用ネットワーク技術16、UPS等の関連機器17、Raid等のミラーリング18、ファイヤーウォールやIDS名等のセキュリティ対策情報19等が格納される。

【0027】

図1に示すシステム管理者情報8には、監視対象システム6の管理者（図1に21で示す）の氏名、その情報提供先アドレスが格納される。組織情報9には、前記管理者21が属する組織の名称及びその組織の管理者（経営者；図に22で示す）の氏名及び情報提供先アドレスが、前記システム管理者情報8に関連付けて格納される。

【0028】

脆弱点修正情報10は、前記システム管理者21が脆弱点情報に基づいて施した脆弱点修正作業のログが、システム毎に記録されてなるものである。前記セキュリティレベル値11は、図3に示すように、セキュリティ基準値11aと、セキュリティレベル値履歴11bと、内的要因ポイント11cからなる。セキュリティ基準値11aは、組織の経営者（組織管理者22）に対してその組織のセキュリティレベルを示すための基準値であり、予め当該組織でセキュリティに関する事故が発生した場合の損害や株価の影響などを考慮して決定され格納される。また、セキュリティレベル値履歴11bには、過去に算出したセキュリティレベルが履歴として格納される。内的要因ポイント11cは、後で詳しく説明するようにセキュリティレベル値を求めるために用いるものである。

【0029】

一方、脆弱点DB3には、脆弱点情報4として、図4に示すように、脆弱点の概要情報を含む脆弱点概要情報25と、当該脆弱点による脅威について記述した脅威情報26と、当該脆弱点を修正するための脆弱点パッチ情報27と、前記修正を実際のシステムで検証した結果を記述する脆弱点検証情報28と、各脆弱点情報の脅威に関して重み付けをするための脅威レベル値29が格納されている。

これらの情報の生成は、図5に示すように、このシステム1の運営者が、まず、外部ベンダーから主に英語で提供された脆弱点情報やパッチ情報を収集、翻訳し（ステップS1）、技術的な検証をする（ステップS2）。そして、各脆弱点情報に独自の脅威レベル値29を付し（ステップS3）、前記脆弱点DB3を更新する（ステップS4）。このDB3の更新は、前記DB更新部5を通して行う。

【0030】

一方、前記脆弱点監視処理部4は、図1に示すように、このシステム1にアクセスするユーザの認証を行うユーザ認証部30と、システム管理者21等から環境情報7及び管理者情報8の入力を受け付けてこれらを更新する環境情報／管理者情報／組織情報登録部31と、前記脆弱点DB3から脆弱点情報24を取り出して前記システム管理者21に提供する脆弱点情報提供部32と、システム管理者21からこのシステム管理者21が前記脆弱点情報24に基づいて施した修正作業記録の入力を受取り前記脆弱点修正情報10として記録する脆弱点修正作業ログ記録部33と、この修正情報10に基づいて脆弱点对策情報を生成し、前記組織の管理者（経営者22）にレポートする脆弱点对策情報作成部34と、前記脆弱点情報24とこれに対する修正情報10に基づいて当該組織のセキュリティレベルを算出するセキュリティレベル算出部35と、算出したセキュリティレベルに基づく情報を前記組織管理者（経営者22）に提供するセキュリティレベル情報作成部36とを有する。

【0031】

これらの構成要素は、実際には、一般的なコンピュータシステムに設けられたハードディスク等の記憶媒体にインストールされた1又は2以上のコンピュータソフトウェアプログラムによって実現され、このコンピュータソフトウェアプログラムは前記コンピュータシステムのCPUによってRAM上に呼び出され適宜実行されることでこの発明の機能を奏するようになっている。

【0032】

以下、上記構成要素の構成及び機能の詳しい説明を、図6以下の画面構成図に基づき、実際の動作を参照して説明する。

【0033】

図6は、このシステム1へのログイン画面の例である。

【0034】

例えば、前記システム管理者21が前記システム1に接続する場合、自己の端末からインターネット等を通して接続し、このログイン画面を立上げる。そして、このログイン画面のユーザ名入力ボックス40およびパスワード入力ボックス41にそれぞれ必要な情報を入力し、「Go」ボタン42を押す。このことで、前記ユーザ認証部30が当該システム管理者21の認証を行い、この監視システム1への接続を確立する。

【0035】

接続者がシステム管理者21である場合、前記脆弱点情報提供部32が前記の認証結果に従い、図7に示す画面を前記システム管理者21の端末上に表示させる。この画面には、修正ソフトウェアの適用を推奨するコンピュータ群44が表示されている。このような表示を行わせるためには、前記監視対象コンピュータシステム6の環境情報7が前記ユーザシステムDB2に適切に登録されている必要がある。この環境情報の入力及び更新を行うには、この図7の画面の環境登録ボタン45を押す。

【0036】

このボタン45が押されると、前記環境情報／管理者情報／組織情報登録部31が、図8に示す画面を表示する。システム管理者21はこの画面を通してこの監視対象のコンピュータシステムの環境情報を入力することができる。この実施例では、この画面のコンピュータリスト46に示されるように、このシステム管理者21の属する組織は、東京本社と名古屋工場とを有し、東京本社には監視対象としてMA-T1、MA-T2、MA-T3の3台のコンピュータが、名古屋工場にはMA-N1、MA-N2、MA-N3の3台のコンピュータがそれぞれ設けられネットワークに接続されている。

【0037】

この画面に示すのは、このうちMA-T1に関するシステム環境情報である。この画面を通し、図2で説明した各情報12～19を各システム毎に入力していく。ここで、システム管理者の登録は必須であり、このシステム管理者情報の編

集はこの図に47で示す管理者登録ボタンを押すことによって行えるようになっている。

【0038】

また、この実施形態においては、この画面に、自動診断ボタン48が設けられており、この自動診断ボタン48を押すことで、前記した各情報を自動的に監視対象コンピュータシステム6から取得することができるようになっている。すなわち、図1に示すように、前記コンピュータシステム6には、このコンピュータシステム6の環境情報を取得する環境情報取得システム60が接続されている。そして、前記ボタン48が押されることで、前記前記環境情報／管理者情報／組織情報登録部31が前記環境情報取得システム60を起動して前記コンピュータシステム6の環境情報の全て若しくは一部を取得させることができるようになっている。

【0039】

脆弱点情報提供部32は、システム管理者21がこの脆弱点監視システム1にアクセスして来たならば、上記のようにして登録されたユーザシステムDB2内の環境情報7と前記脆弱点DB3内の脆弱点情報24とのマッチングを行う。そして、この脆弱点DB3内に前記システム6のハードウェア構成等に適合する脆弱点情報24があったならば、このコンピュータをセキュリティ対策の必要なコンピュータとしてピックアップして、図7に示す画面の符号44で示す一覧に表示する。この例では、前記した全てのコンピュータが、脆弱点修正の必要なコンピュータシステムとしてピックアップされている。このことで、各脆弱点情報24が各監視対象のコンピュータシステムに関連付けられることになる。

【0040】

システム管理者21は、この画面から、脆弱点一覧ボタン49を押すことで図9に示すように脆弱点一覧50を閲覧することができる。この脆弱点の一覧表示は、前記属性情報12に基づき、システム種別を基準として表示することもできるし、OSを基準として表示することもできるし、ロケーションを基準として表示することもできる。そして、この画面から各脆弱点をクリックすることで、さらに詳細な情報にアクセスすることができる。この場合、前記脆弱点情報提供部

32は、前記脆弱点DB3から図3に示す25～28の各詳細情報を取り出し、図10に示すように表示する。

【0041】

このことでこのシステム管理者21はこの脆弱点の詳細を確認し、対策の要否を検討することが可能になる。この脆弱点を確認した後、この対策を採った場合には、この画面の作業ログボタン51を押すことで、脆弱点修正作業の記録の入力を行う。

【0042】

図11は、この作業ログの入力画面である。この画面には、選択に係る脆弱点の修正に必要な作業が時系列的に列挙されており、システム管理者21は、各必要な作業を採ったかを確認し、実施日を入力していく。

【0043】

このように入力された脆弱点修正作業は、前記脆弱点修正作業ログ記録部33によって前記ユーザシステムDB2内に前記脆弱点修正情報10として格納される。そして、図11に列挙された全ての作業が終了した場合には、この対応が済んだものとして記録されることになる。なお、この画面には、「対象外」ボタン52と、「暫定措置」ボタン53が設けられている。前記脆弱点情報が当該システムに対応しないものであるときには、この対象外ボタン52を押すことで処理済みとすることができる。また、暫定措置ボタン53は、脆弱点に対応する有効なパッチが提供されておらず、後で対応する場合等に使用する。

【0044】

次に、前記組織管理者22がこの脆弱点監視システム1に接続する場合について説明する。

【0045】

前記組織管理者22がこのシステムにログインした場合、前記ユーザ認証部30は、前記組織情報9に基づいて、組織管理者22であることを検出する。このことに基づき、前記脆弱点情報提供部32は、図12に示すように、組織管理者22向けに、脆弱点対策情報を生成して提示する。この脆弱点対策情報は、この画面に示されるように、例えば、管理者毎、システム毎に、脆弱点情報と、その

情報の発効日、対策を採った対応日を含む。対策をとった対応日は、前記修正情報 10 から取得して表示されることになる。また、未だ対策をとっていない脆弱点に基づき、前記脆弱点 DB 3 から、脅威情報 26 等を取り出し、この画面に 54 で示すように表示する。

【0046】

このような画面により、組織管理者 22 は、自己の組織に係るネットワーク若しくはこのネットワークに接続されたコンピュータシステムのセキュリティ管理状況を確認することが可能になる。また、このシステムは、システム管理者 21 の採った修正作業を記録しておき、これを組織管理者 22 に提示するようにしたから、この組織管理者 22 は、システム管理者 21 を適切に管理することができる。

【0047】

また、図 12 の画面から、改善状況の表示ボタン 55 を押すと、前記セキュリティレベル算出部 35 が起動し、各脆弱点毎のセキュリティレベルを算出する。また、このセキュリティレベル算出部 35 は、脆弱点間、コンピュータ間のセキュリティレベル値を比較してコンピュータ毎及びネットワーク毎のセキュリティレベル値を算出するためのセキュリティレベル値比較部 59 を有する。

【0048】

図 13 に示すように、前記セキュリティレベルは、第 1 のグラフ 56 と第 2 のグラフ 57 の 2 つのグラフで示される。

【0049】

第 1 のグラフ 56 は、修正プログラム適用率である。各脆弱点情報の発効日付別に、適用した修正プログラムの数が、棒グラフで示されている。このグラフは、発効日を基準とするから、先月発効した脆弱点情報は、当月に修正作業を行ったとしても、先月分としてカウントされる。

【0050】

第 2 のグラフ 57 は、前記修正結果に基づく、セキュリティレベルの変化を示す折れ線グラフである。以下、この第 2 のグラフ 57 の表示手順について説明する。

【0051】

まず、この実施形態では、セキュリティレベルは、「内的要因」、「外的要因」及び「その他」からなるものと定義される。

【0052】

内的要因とは、セキュリティポリシーの有無や日々の運用状況、ネットワーク構成やセキュリティ機器の設置、設置状況等により評価される静的な値である。この内的要因は、例えば、3月若しくは半年に一回、セキュリティコンサルタントがチェックシートによって行った評価により導き出される。

【0053】

外的要因とは、日々新たに発見される脆弱点情報により求められる動的な値である。この外的要因は、基本的に、脆弱点情報の対象となっている機器の種別、前記脆弱点情報中の脅威レベル値、この脆弱点情報が発効してから何日経過しているかの情報に基づいて、前記組織管理者がアクセスする毎に算出される。

【0054】

セキュリティレベルの算入割合は、内的要因を70パーセント、外的要因を20パーセント、その他を10パーセントとする。ただし、その他は、人為的なミス等を表しているので、この実施形態では評価対象外とする。したがって、この実施形態では、内的要因の最高値70ポイント、外的要因の最高値20ポイントの合計最高点90ポイントとしてセキュリティレベル値を算出する。なお、前述したように、内的要因ポイントは、予め算出され、前記ユーザシステムDB2内に格納されている。

【0055】

図14は、前記セキュリティレベル算出部35によるセキュリティレベル値算出工程を示すフローチャートである。

【0056】

この実施形態では、ネットワーク全体のセキュリティレベルを導き出すのに、まず、図14のステップS5～S9で、このネットワークに属する複数のコンピュータ毎のセキュリティレベルを算出する。そして、ステップS10～S14で、このコンピュータ毎のセキュリティレベルを比較し最低のものをネットワーク

のセキュリティレベルとして採用する。

【0057】

このため、前記セキュリティレベル算出部35は、まず、ネットワークに属する複数のコンピュータのうちの1番目（ $n=1$ ）のコンピュータの1番目の脆弱点情報から処理を開始する（ステップS5）。

【0058】

そして、ユーザシステムDB2から、当該コンピュータ（機器）の種別情報、前記脆弱点情報の脅威レベル値、この脆弱点情報が発行してから何日経過しているかの情報を取得し（ステップS6）、以下の式により、この脆弱点情報に関する外的要因ポイント値 wpp を算出する（ステップS7）。

【0059】

$$Wpp = 2.0 + hp \times hk \times il \times date$$

- ・ここで Wpp は、値が低いほど脅威が大きいことを意味する。
- ・ hp は、基準パラメータであり、ここでは-1とする。
- ・ hk は、コンピュータ種別（機種種別）であり、セキュリティ機器については2点、その他の機器については1点とする。
- ・ il は当該脆弱点情報に付加された前記脅威レベル値（図4の符号29参照）であり、三段階に設定され、Sは4点、Aは2点、Bは1点とされている。
- ・ $date$ は、これまでに対応せずに経過した日数であり、前記脆弱点情報が発効した日と現在との差により求める。

【0060】

この外的要因ポイント値 wpp を、当該システムに適用された全ての未対応の脆弱点について求め（ステップS8）、その中で、最も値の小さいものを、当該コンピュータシステムの外的要因ポイント値 $wpp(n)$ として出力する（ステップS9）。

【0061】

また、当該組織内のネットワークに属する全てのコンピュータシステムに対しても、同様に外的要因ポイント値 $wpp(n)$ を求めていく（ステップS10）。このようにして、全てのコンピュータシステムについての処理が終了したなら

ば、ネットワーク中で最小のwppを、ネットワーク全体の外的要因ポイント値wpp(a11)とする(ステップS11)。

【0062】

ついで、前記セキュリティレベル算出部35は、前記セキュリティレベル値11から内的要因ポイント11cを取得し(ステップS12)、これに、前記外的要因ポイントwpp(n)及びwpp(a11)を加算することで、セキュリティレベル値(SP)を算出する(ステップS13、S14)。

【0063】

次に、前記セキュリティレベル情報作成部36が、セキュリティレベル値SPと前記セキュリティ基準値11a及びセキュリティレベル値履歴11bを用いて図13に示す第2のグラフ57を作成する(ステップS15)。

【0064】

すなわち、この実施形態では、前記セキュリティレベル情報作成部36は、前記セキュリティレベル値履歴11bから、過去1年間の各月の末日のセキュリティレベル値を取り出し、それを各月のセキュリティレベル値とする。そして、現在求めたセキュリティレベル値SPを当月のセキュリティレベル値とする。そして、これらのセキュリティレベル値を、図13に示すように、前記セキュリティ基準値を中心値とする折れ線グラフ57として表示する。

【0065】

このような折れ線グラフによれば、専門知識の少ない経営者であっても、当該組織のセキュリティレベル値を一目で評価することが可能になる。

【0066】

なお、この発明は、上記一実施形態に限定されるものではなく、発明の要旨を変更しない範囲で種々変形可能である。

【0067】

例えば、上記一実施形態では、システム管理者及び組織管理者は、インターネット等を通して前記脆弱点監視システムから各種情報を受け取るようにしたが、これに限定されるものではない。例えば、E-mail等の手段で各種情報を提供するようにしても良い。

【0068】

また、前記セキュリティレベルの表示は、棒グラフ及び折れ線グラフで行うようにしたが、これに限定されるものではなく、具体的な数値を示すことで行なうようにしても良い。さらに、前記セキュリティレベルの具体的な算出方法は、この発明の要旨の範囲で種々変更可能である。例えば、内的要因ポイント利用せず、外的要因ポイント wpp 、 $wpp(n)$ 、 $wpp(all)$ により求めたセキュリティレベルのみを提供するようにしても良い。

【0069】

【発明の効果】

以上説明した構成によれば、セキュリティに関して十分な知識を有さない者であっても理解できるようなセキュリティ情報を簡便な構成で迅速に提供することができる。

【図面の簡単な説明】

【図1】

この発明の一実施形態を示す概略構成図。

【図2】

コンピュータシステム環境情報の構成を説明するための図。

【図3】

セキュリティレベル値の構成を説明するための図。

【図4】

脆弱点情報の構成を説明するための図。

【図5】

脆弱点DBの更新工程を示す工程図。

【図6】

ログイン画面を示す図。

【図7】

システム管理者に対する情報提供画面を示す図。

【図8】

環境情報登録画面を示す図。

【図 9】

脆弱点情報の一覧画面を示す図。

【図 10】

脆弱点情報の詳細画面を示す図。

【図 11】

脆弱点修正作業の入力画面を示す図。

【図 12】

組織管理者に対する情報提供画面を示す図。

【図 13】

組織管理者に対するセキュリティレベル情報の提供画面を示す図。

【図 14】

セキュリティレベル値の算出工程を示すフローチャート。

【符号の説明】

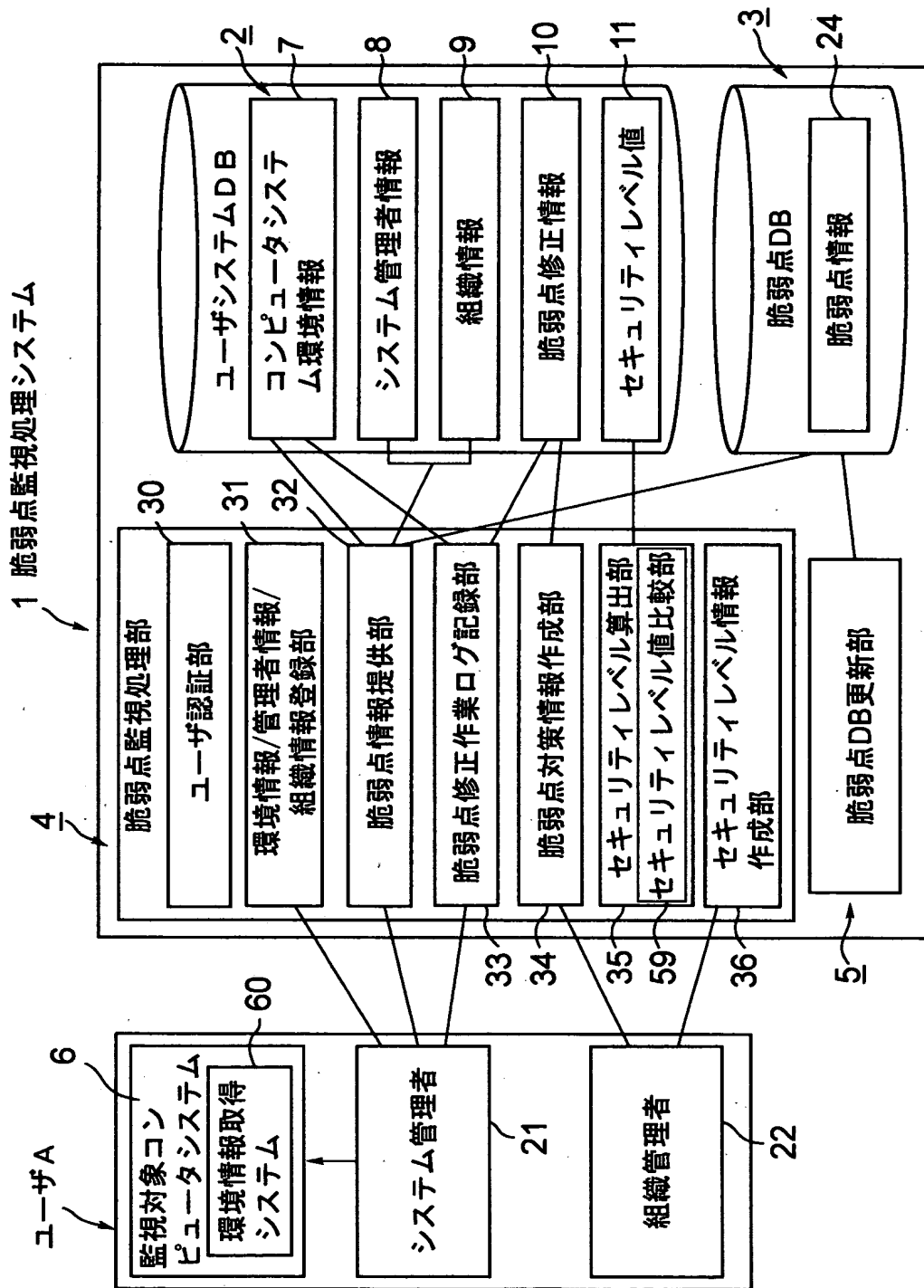
- 1 …脆弱点監視システム
- 2 …ユーザシステムDB
- 3 …脆弱点DB
- 4 …脆弱点監視処理部
- 5 …DB更新部
- 6 …監視対象コンピュータシステム
- 7 …コンピュータシステム環境情報
- 8 …システム管理者情報
- 9 …組織情報
- 10 …脆弱点修正情報
- 11 …セキュリティレベル値
 - 11a …セキュリティ基準値
 - 11b …セキュリティレベル値履歴
 - 11c …内的要因ポイント
- 12 …属性情報
- 13 …ハードウェア構成

- 14…ソフトウェア構成
- 15…設定
- 16…利用ネットワーク技術
- 17…関連機器
- 18…ミラーリング
- 19…セキュリティ対策情報
- 21…システム管理者
- 22…組織管理者
- 24…脆弱点情報
- 25…脆弱点概要情報
- 26…脅威情報
- 27…脆弱点パッチ情報
- 28…脆弱点検証情報
- 29…脅威レベル値
- 30…ユーザ認証部
- 31…環境情報／管理者情報／組織情報登録部
- 32…脆弱点情報提供部
- 33…脆弱点修正作業ログ記録部
- 34…脆弱点対策情報作成部
- 35…セキュリティレベル算出部
- 36…セキュリティレベル情報作成部
- 56…第1のグラフ
- 57…第2のグラフ
- 59…セキュリティレベル値比較部
- 60…環境情報取得システム

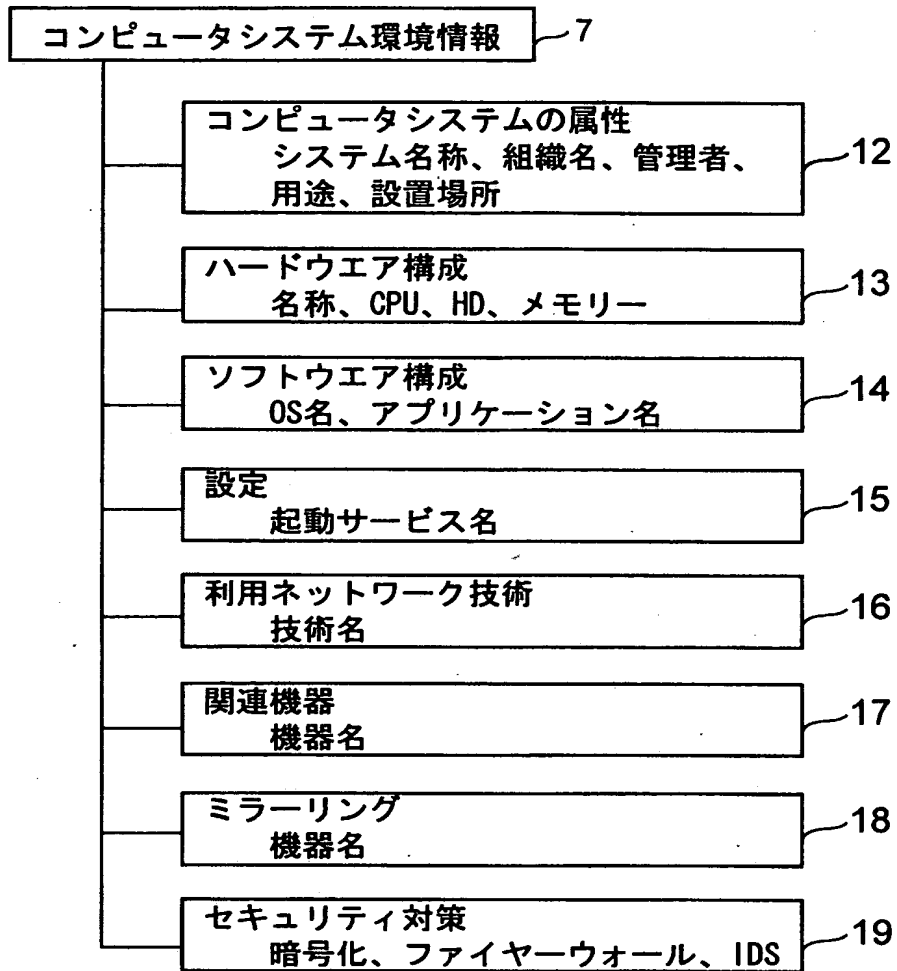
【書類名】

図面

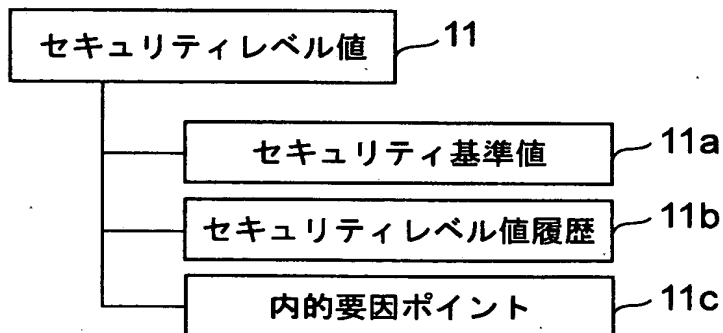
【図 1】



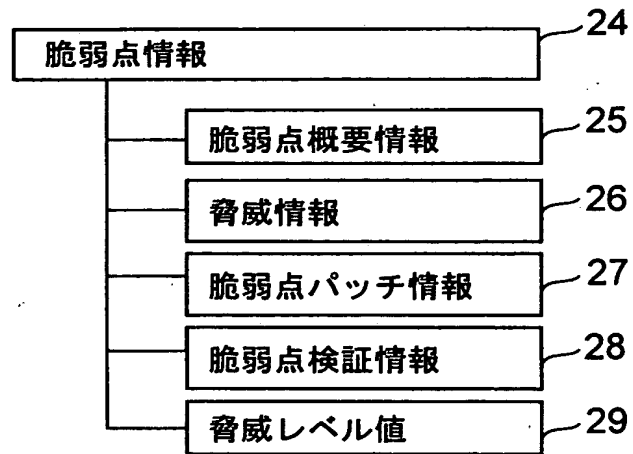
【図 2】



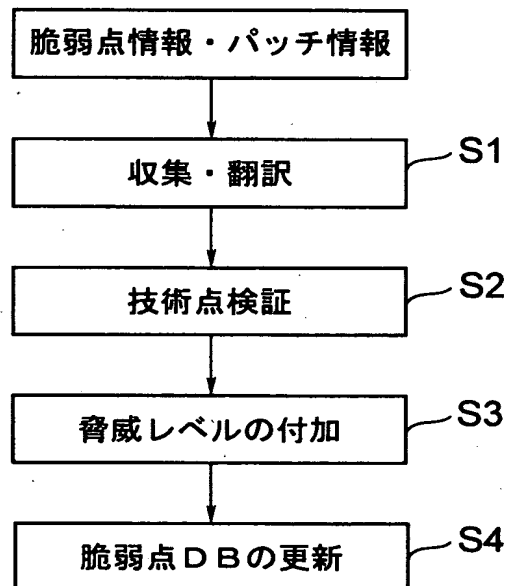
【図 3】



【図 4】



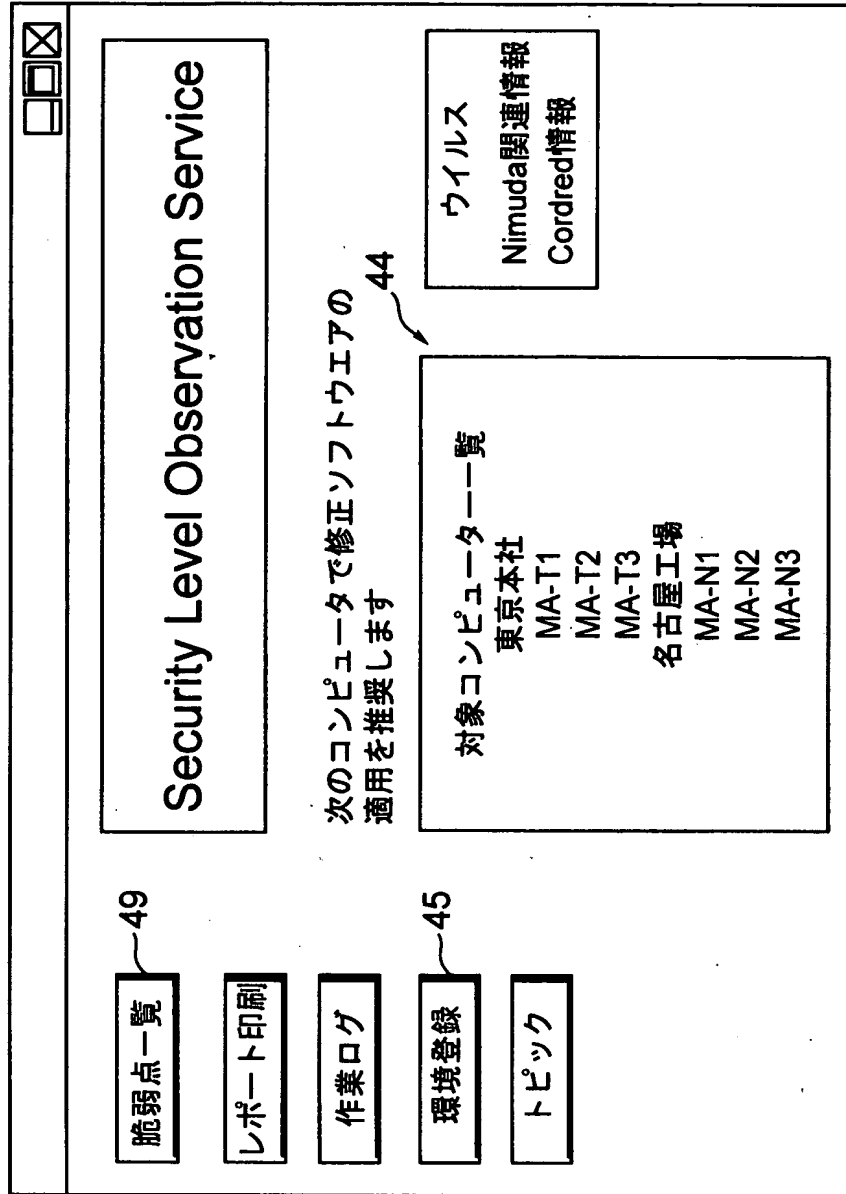
【図 5】



【図 6】

The diagram shows a login window with a title bar at the top. The title bar contains the text "ログイン" (Login) on the left and three standard window control icons (minimize, maximize, close) on the right. The main area of the window contains two vertical input fields. The left field is labeled "Username" and is identified by reference numeral 40. The right field is labeled "Password" and is identified by reference numeral 41. To the right of the Password field is a button labeled "Go", identified by reference numeral 42.

【図 7】



【図 8】

12

<div style="text-align: right;"> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div>					
<p>46</p> <p>マシンから選択 東京本社 MA-T1 MA-T2 MA-T3 名古屋工場 MA-N1 MA-N2 MA-N3</p>	<table border="1"> <tr> <td> <p>名称 MT-T1 所属 東京本社 管理者 日本 太郎 用途 Mail Server</p> </td> <td> <p>設置場所 東洋本社5F DMZ 外部公開</p> </td> </tr> <tr> <td> <p>・ハードウェア構成</p> <p>名称 CPU HD Memory テープバックアップ ・ソフトウェア構成</p> <p>OS AP sendmail ウイルスXXX for server ・設定 起動サービス ports ipfilter ntp server 125 ・利用ネットワーク技術 OCN-3 ・関連機器 UPS 名称 ・ミラーリング Raid</p> </td> <td> <p>・セキュリティ対策</p> <p>暗号化 HD暗号化 有無 認証 ssh firewall情報 名称 設定 IDS 名称 通過プロトコル</p> </td> </tr> </table>	<p>名称 MT-T1 所属 東京本社 管理者 日本 太郎 用途 Mail Server</p>	<p>設置場所 東洋本社5F DMZ 外部公開</p>	<p>・ハードウェア構成</p> <p>名称 CPU HD Memory テープバックアップ ・ソフトウェア構成</p> <p>OS AP sendmail ウイルスXXX for server ・設定 起動サービス ports ipfilter ntp server 125 ・利用ネットワーク技術 OCN-3 ・関連機器 UPS 名称 ・ミラーリング Raid</p>	<p>・セキュリティ対策</p> <p>暗号化 HD暗号化 有無 認証 ssh firewall情報 名称 設定 IDS 名称 通過プロトコル</p>
<p>名称 MT-T1 所属 東京本社 管理者 日本 太郎 用途 Mail Server</p>	<p>設置場所 東洋本社5F DMZ 外部公開</p>				
<p>・ハードウェア構成</p> <p>名称 CPU HD Memory テープバックアップ ・ソフトウェア構成</p> <p>OS AP sendmail ウイルスXXX for server ・設定 起動サービス ports ipfilter ntp server 125 ・利用ネットワーク技術 OCN-3 ・関連機器 UPS 名称 ・ミラーリング Raid</p>	<p>・セキュリティ対策</p> <p>暗号化 HD暗号化 有無 認証 ssh firewall情報 名称 設定 IDS 名称 通過プロトコル</p>				

自動診断

管理者登録へ

48

47

【図 9】

50

<div><div><div></div><div></div><div></div></div></div>		<div>条件検索 全て 未対応 対応済み G0</div>	
<div>マシンから選択 東京本社 MA-T1 MA-T2 MA-T3 名古屋工場 MA-N1 MA-N2 MA-N3 OSから選択 UNIX 東京本社 MA-T1 MA-T2 MA-T3 名古屋工場 Windows 東京本社 名古屋工場 MA-N1 MA-N2 MA-N3</div>			
<div>MA-T1の脆弱点</div> <div><div><div><input type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div><div><div><input checked="" type="checkbox"/> RSA advisory</div><div>NOXXXXX</div><div>ストリングフォーマットについて</div></div><div><div><input type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div><div><div><input type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div></div>			
<div>MA-T2の脆弱点</div> <div><div><div><input type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div><div><div><input checked="" type="checkbox"/> RSA advisory</div><div>NOXXXXX</div><div>ストリングフォーマットについて</div></div><div><div><input type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div><div><div><input checked="" type="checkbox"/> CERT advisory</div><div>NOXXXXX</div><div>LPD脆弱点について</div></div></div>			
<div><input checked="" type="checkbox"/> マゼンダは未対応 <input type="checkbox"/> 青は対応</div>			

【図 10】

<div> <div> <div></div> <div></div> <div></div> </div> </div>				
マシンから選択	表示条件検索	全て	概要のみ	技術的情報
東京本社	CERT advisory	NOXXXXX	LPD脆弱点について	
MA-T1	登録日	2001年12月1日		
MA-T2	更新日			
MA-T3	概要	UNIXのシステムのラインプリンターデーモンにリモートから…		
名古屋工場		の脆弱点があります。		
MA-N1		影響		
MA-N2		S		
MA-N3		ルート権限を奪われる可能性があります。		
OSから選択		推奨する対策		
UNIX		技術的解説		
東京本社		修正プログラム入手方法		
MA-T1		インストール手順		
MA-T2		リンク情報		
MA-T3		更新履歴		
名古屋工場				
Windows				
東京本社				
名古屋工場				
MA-N1				
MA-N2				
MA-N3				
作業ログへ		51		

【図 1 1】

マシンから選択 東京本社 MA-T1 MA-T2 MA-T3 名古屋工場 MA-N1 MA-N2 MA-N3 OSから選択 UNIX 東京本社 MA-T1 MA-T2 MA-T3 名古屋工場 Windows 東京本社 名古屋工場 MA-N1 MA-N2 MA-N3 脆弱点一覧へ		MT-T1 東京本社 CERT advisory NOXXXXX LPD脆弱点について
<input checked="" type="checkbox"/> 内容の確認	実施日	2001/12/07
<input checked="" type="checkbox"/> 修正プログラム入手		2001/12/07
<input checked="" type="checkbox"/> テスト環境で動作確認完了		2001/12/07
<input type="checkbox"/> 実施計画検討		
<input type="checkbox"/> バックアップ実施		
<input type="checkbox"/> 関係者へのアナウンス完了		
<input type="checkbox"/> 実行環境での動作確認		
<input type="checkbox"/> 完了アナウンス完了		
	52 対象外	53 暫定処置

【図 12】

管理責任者

日本太郎

所属

東京本社

改善状況

55

MA-T1の脆弱点

対応

件名

発行日

対応日

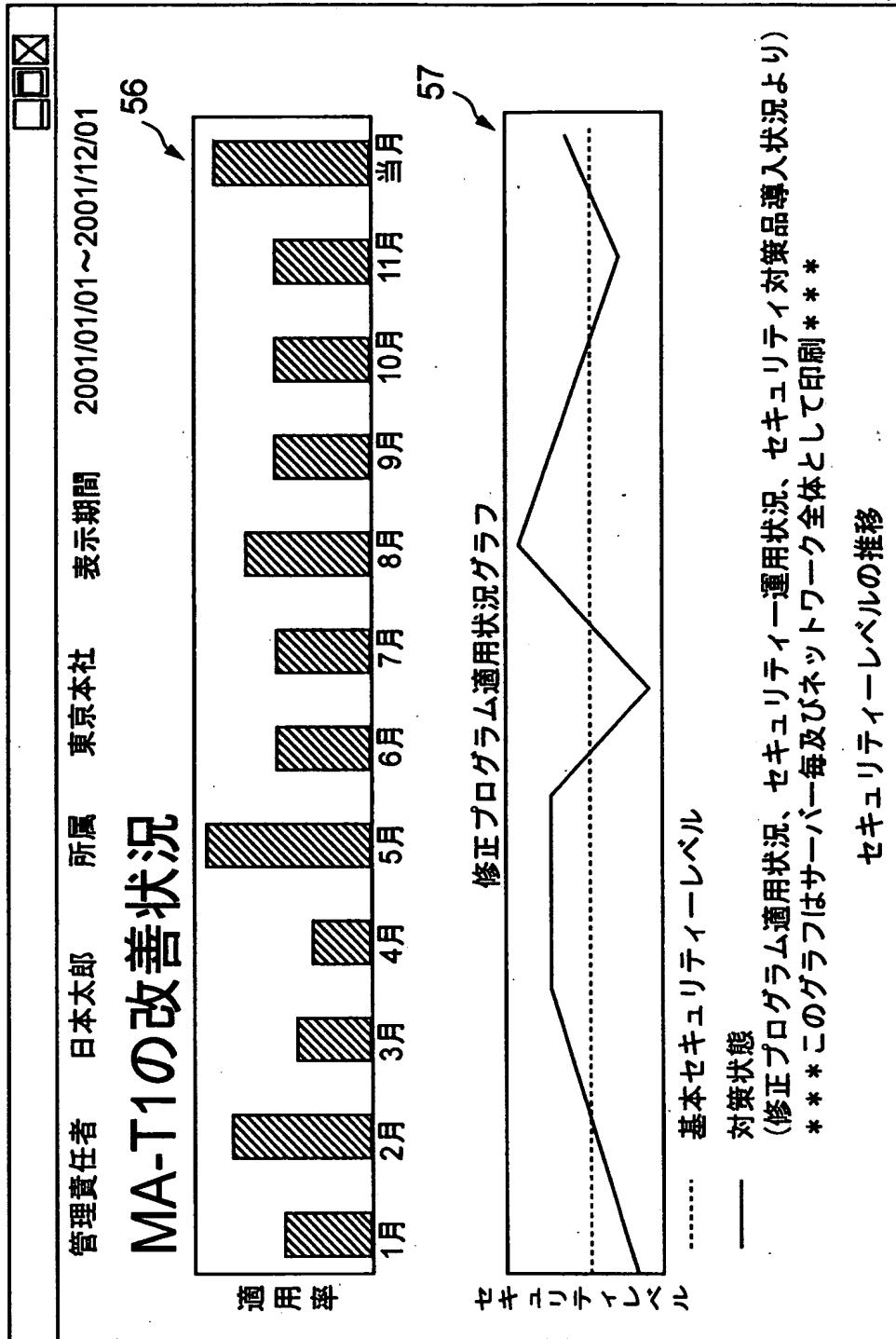
<input type="checkbox"/> CERT advisory NOXXXXX	LPD脆弱点について	2001/12/07	
<input type="checkbox"/> RSA advisory NOXXXXX	ストリングフォーマットについて	2001/12/07	2001/12/10
<input type="checkbox"/> CERT advisory NOXXXXX	LPD脆弱点について	2001/12/07	
<input type="checkbox"/> CERT advisory NOXXXXX	LPD脆弱点について	2001/12/07	2001/12/10

☐ マゼンダは未対応 ☐ 青は対応

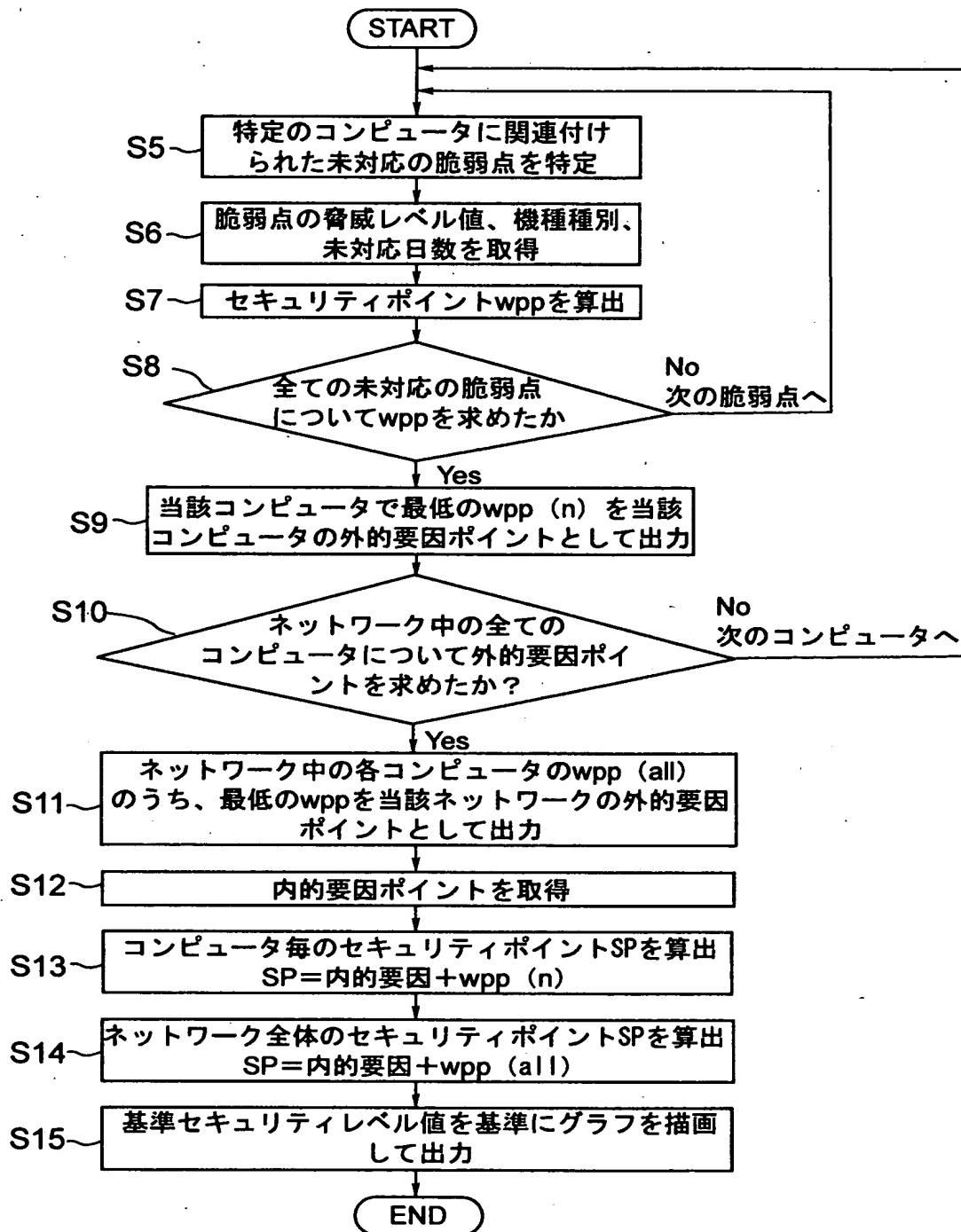
MA-T1への考えられる攻撃・脅威

修正ソフトウェア更新状況について
バックドアオーバーフロー攻撃
LPDに存在するバックドアオーバーフローの脆弱点を突いた攻撃でルート権限を奪取される可能性がります。最悪、侵入、情報漏洩にいたり致命的な障害に発展する可能性があります。
セキユリティ運用状態について
DDOS攻撃対策を行っていません。意識しないうちにspamメールの送信者としてリストアップされる可能性がります。お客様からの信用の失墜や第3者からのクレームを受けたり公的機関からの問い合わせを受けることも考えられます。

【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 セキュリティ技術に関して十分な知識を有さない者であっても理解できるように処理されたセキュリティ情報を提供する。

【解決手段】 少なくとも脆弱点の脅威レベル値を含む情報を格納する脆弱点情報格納部と、監視対象コンピュータシステムの環境情報に基づいて当該コンピュータシステムに適用すべき脆弱点情報を前記脆弱点情報格納部から抽出し、このコンピュータシステムに関連付ける脆弱点情報提供部と、この脆弱点情報に基づいてシステムの管理者が修正作業を行ったかの情報を格納する脆弱点修正情報格納部と、特定の機器について、その種別、この機器について未だ対策を採っていない脆弱点の脅威レベル値、未対応日数から当該機器の当該脆弱点に関するセキュリティレベル値を算出するセキュリティレベル算出部とを有する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2002-010888
受付番号	50200065059
書類名	特許願
担当官	末武 実 1912
作成日	平成14年 2月 5日

<認定情報・付加情報>

【提出日】 平成14年 1月18日

【特許出願人】

【識別番号】 501006882

【住所又は居所】 東京都品川区上大崎3丁目14番37号

【氏名又は名称】 株式会社チームガイア

【代理人】 申請人

【識別番号】 100104215

【住所又は居所】 東京都港区南青山2丁目13番7号 マトリス4
F 大森・矢口国際特許事務所

【氏名又は名称】 大森 純一

【選任した代理人】

【識別番号】 100104411

【住所又は居所】 東京都港区南青山2丁目13番7号 マトリス4
F 大森・矢口国際特許事務所

【氏名又は名称】 矢口 太郎

出 願 人 履 歴 情 報

識別番号 [501006882]

1. 変更年月日 2001年10月30日
[変更理由] 住所変更
住 所 東京都品川区上大崎3丁目14番37号
氏 名 株式会社チームガイア